REMARKS

Claims 29-144 are pending in the instant application. The Examiner maintains his rejection of Claims 1, 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 under 35 U.S.C. §102(e), stating that said claims are being anticipated by U.S. Patent No. 6,289,323 B1 (Gordon et al.)(hereinafter, "Gordon")[1]. Claims 38 and 52 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gordon in view of U.S. Patent No. 5,337,358 A)(Axelrod et al.)(hereinafter, "Axelrod"). Claims 65-71, 86-91 and 128-132 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The Examiner states that he has fully considered Applicants' remarks filed in their Response dated May 16, 2005 (hereinafter, "May 16th Response"), but that said remarks are not persuasive. Applicants incorporate said remarks by reference herein, and further completely and fully address the Examiner's reply to said remarks. Therefore, for the reasons set forth herein and previously, Applicants respectfully submit that claims 29-144 are patentable over the cited art.

I. As Applicants Clearly Set Forth the Definition for the Limitation "Critical Document Data" in the Specification of the Subject Application, Examiner's Continued Objection is Erroneous (Claims 29-144)

The Examiner continues to object to the claimed limitation "critical document data" as a term with relative meaning and thus possible of creating ambiguity. The Examiner's objection is erroneous for at least the following reasons.

It is well established that a patentee is his own lexicographer. *See, e.g., Universal Oil*, 137 F.2d 3, 6 (7th Cir. 1943), aff'd, 322 U.S. 471 (1944). Should the definition ascribed by the patentee to the term or terms used in the claim differ from the standard definition, the differing definition must be clearly set forth in the specification. *Beachcombers Int'l, Inc. v. WildeWood Creative Prods., Inc.*, 31 F.3d 1154, 1158, 31 USPQ2d 1653, 1656 (Fed. Cir. 1994) ("As we have repeatedly said, a patentee can be his own lexicographer provided the patentee's definition, to the extent it differs from the conventional definition, is clearly set forth in the specification.")

[1] Applicants would note that, as acknowledged by the Examiner at page 2 of the Final Office Action, claim 1 has been previously canceled. Therefore, the §102(e) rejection as against this claim has been rendered moot.

The Examiner bases his objection in large part on a subtitle found at page 15, lines 15-19, stating that the Applicants have defined "*'critical document data' as [a] 'personal value document having digital signature.'*" (Final Office Action, p. 2). The Examiner further contends that "*it is not clear if 'critical document data' have digital signatures or not*", and that "*one of ordinary skill in the art would not define 'critical document data' necessary [sic] having an embedded digital signature....*" (*Id. at* p. 3) However, a careful review of the ***entire*** specification, and particularly that encompassed by this subtitle, places it into context and reveals that the Examiner misinterprets the meaning of the subtitle as well as the meaning of "critical document data." More specifically, the subtitle, *in toto*, reads "A. Personal Value Document Having Digital Signature 1 (Critical Document Data), Digital Signature 2 (Critical Document Data and PIN) and Public Key Certificate." A thorough review of the applicable sections reveals that the embodiment of the invention disclosed therein is drawn to a Personal Value Document having: a first digital signature (digital signature 1) that is applied against the "critical document data;" a second digital signature (digital signature 2) that is applied against both the "critical document data" and a PIN (wherein the "critical document data" and the PIN are an "authenticatable data string"); and a public key certificate. (*09/707,433 Application*, pp. 15-18). Thus, the Examiner's contention that "critical document data" is a "personal value document having digital signature" is erroneous.

Furthermore, as previously stated in the May 16th Response, Applicants have provided a clear meaning to the term "critical document data" throughout the subject application (*see, e.g., 09/707,433 Application*, pp. 16-17). In particular, the application sets forth the following:

> *1. Critical Document Data*
>
> *In accordance with the preferred embodiment of the present invention, MICR code line 90 is designated as critical document data (FIG. 5). It is this critical document data that is targeted for enhanced security. (It will be appreciated that as there may be other data printed on a personal check 45 that are known at the time of printing, such as account name and address 92, which may are also be designated as part of that critical document data, and the scope of the present invention includes such data).*
>
> *In one aspect of a preferred embodiment of this invention, the entire preprinted MICR code line 90, including the special symbols 91 and 93 that identify particular MICR fields, is designated "critical document data"....*
>
> *Optionally, ASCII text strings (e.g., those identifying the account holder's name and address 92 in a personal value document) can also be designated critical document data....*

> *In accordance with another aspect of the preferred embodiment of the present invention, if such ASCII or other data is designated critical document data, it will need to be stored in machine-readable form on personal check 45 in a manner described in more detail in the forthcoming paragraphs. However, when the critical document data is simply the data that is stored in the MICR code line, there is no need to redundantly store this information in an alternate machine-readable format, as MICR characters are already machine-readable.*

(*Id. at* pp. 16-17, lines 5-34; 4-10). That the limitation "critical document data" may have alternate embodiments does not make it ambiguous.

In view of the foregoing, the Examiner's objection with regard to the claimed limitation "critical document data" as a term with relative meaning and thus possible of creating ambiguity cannot stand.

II. That Applicants Use an Identical Public/Private Key Pair for the First and Second Digital Signatures May be Inferred from the Context of Claims 29-42, 75-92 and 100-108 and Well-Known Principles of Public Key Cryptography[2]

In response to Applicants argument that, unlike Gordon, the first and second digital signatures Applicants' claimed invention are created using an identical public/private key pair, the Examiner maintains that this limitation is not recited in the subject claims, and may not be read into the claim from the specification (Final Office Action, p. 3). The Examiner's argument is in error for at least the following reason:

As further set forth in the subject application, it is known to those of ordinary skill in the public key cryptographic art that each key pair is composed of a public key and a private key, the public key being made publicly available through any of a various means, while the private key is kept secret/confidential. It is also known that the public and private keys are related in such a way that only the public key which is the companion to the private key of the public/private key pair can successfully verify a message/digital signature combination created using the private key. (*09/707,433 Application*, p. 10, lines 11-14)

As further stated in the application and their May 16th Response, the first and second digital signatures of Applicants' claimed invention are created using an identical private/public key pair. For example, as seen at page 18:

[2] Applicants note that they erroneously applied this argument against claims 43-64 and 72-74 in their May 16th Response, and withdraw same. However, the remaining arguments for the patentability of these claims set forth therein are maintained here; namely the argument set forth in IIIC2 - Public Key Certificate, Including Public Key Stored on Document.

> *In the preferred embodiment of the present invention, the check printer 48 assembles the critical document data string, and then calculates a digital signature for the critical document data string (hereinafter, "digital signature 1") using the check printer's private signing key (discussed below). In addition, the check printer 48 assembles the authenticatable data string, and then calculates a second digital signature for the authenticatable data string (hereinafter, "digital signature 2") also using the check printer's private signing key (discussed below).*

(*Id. at* p. 18, lines 13-16) (Emphasis added). Since an identical private key pair is used to create the first and second digital signatures, the principles of public key cryptography dictate that the same public key must be used to verify the digital signature.

Independent claims 29, 75 and 100 clearly indicate this feature. For example, claim 29 recites, in pertinent part:

> *29. A self-authenticating document having critical document data, comprising:*
> *a first digital signature...*
> *a second digital signature...*
> *a public key certificate including an authentic public key for validating said first and second digital signatures wherein said first digital signature, said second digital signature, and said public key certificate are stored on said self-authenticating document.*

(Emphasis added)[3]. As the claimed "authentic public key" validates both the first and second digital signatures, it may be inferred from the public key cryptography principles discussed above that the same private key was used to generate both the first and second digital signatures. Therefore, as both the first and second digital signatures have the same private and public key, the public/private key pairs may be said to be identical, and the Examiner's argument cannot stand.

III. Gordon's Not Only Does Note Teach Including a Public Key Certificate on a Document, but It Specifically Teaches Away from Same (Claims 29-144)

The Examiner sets forth in the Final Office Action that Applicants' arguments that Gordon does not teach or suggest affixing the public key certificate to the document are in error because Gordon's statement that the public key certificate "need not include the public key with the value message" merely means that "*such inclusion is not necessary, and that [it] is an option and not the only solution.*" (Final Office Action, p. 4) Applicants again submit that the Examiner is error for at least the following reasons.

[3] Claims 75 and 100 contains similar claim language, and thus the argument applies as against these claims as well.

At the outset, Applicants would note that the substantial majority of these claims were rejected only under 35 U.S.C. §102(e); that is, the Examiner has not applied a 35 U.S.C. §103(a) obviousness rejection as against the claims.[4] However, in responding to Applicants' arguments regarding this missing limitation, the Examiner fails to address those arguments made against the 35 U.S.C. §102(e) rejection, and merely responds to Applicants' arguments against an anticipated obviousness rejection.

Thus, the Examiner fails to address the initial point raised by Applicants in their May 16th Response that Gordon does not anticipate Applicants' claimed invention under 35 U.S.C. §102(e) because, unlike Applicants' invention, where the public key certificate including the authentic public key is stored on the self-authenticating document itself, the public key of both Gordon's Payer and Payee is obtained via a public "keyring" or database (i.e., not on the value message 14 or 17) For this reason alone, the rejection of claims 29-37, 39-51, 53-64, 72-85, 92-127, and 133-144 under 35 U.S.C. §102(e) cannot stand.

Furthermore, as Applicants argued in their May 16th Response, Gordon does not render obvious Applicants' claimed invention because Gordon's invention specifically ***teaches away*** from Applicants' invention. This may be gleaned from at least the following relevant sections of the Gordon patent. With regard to the Payer device (PSD 12):

> *A PSD certificate serial number 34, provided in barcode form only, identifies the serial number for the certificate used to authenticate the public/private key combination issued to the Payer PSD 12 by a Certificate Authority.* ***The PSD certificate serial number 34 enables the postal authority 10 to select a public key from a public key database maintained by the postal authority 10.*** *The public key corresponds to a private key used by the Payer PSD 12 to create a digital signature for the value message 14.* ***Thus, the Payer PSD 12 need not include the public key with the value message 14.***

[Gordon, Col. 6, lines 45-54](Emphasis added). And, with regard to the Payee device (PSD 16):

> *The endorsed value message 17 includes a set of additional fields for authentication and record keeping. An algorithm ID 52, provided in barcode form only, identifies the type of cryptographic transformation used to render a payee digital signature 54 appended by the Payee PSD 16 when the endorsed value message 17 is issued by the Payee PSD 16.* ***The payee digital signature 54 is cryptographically transformed by means of a public key stored at the postal authority 10 and accessed based upon the payee identification 46.*** *Finally, the endorsed value message 17 includes a date/time 56 which specifies when the Payee PSD 16 issued the endorsed value message 17.*

[Id., Col. 8, lines 29-34](Emphasis added).

[4] With the exception of claims 38 and 52, which were rejected for a separate and unrelated reason.

The sentence apparently at issue is found above at in Gordon at Column 6, lines 53-54:

Thus, the Payer PSD 12 need not include the public key with the value message 14.

Applicants admit that the phrase "*need not*" may be understood in common English usage to mean "not required" or "not necessary," when taken in the abstract. However, Applicants submit that, as seen from the above passages, a careful review of the context in which this phrase is given in Gordon (and in light of the invention itself) reveals that a better interpretation would be that Gordon is stating that as a direct benefit of his invention, the public keys can be stored outside of the message on public keyrings/databases, thus specifically ***avoiding*** the need to include them on the value message 14. Under such interpretation, one skilled in the art would not look to Gordon for teaching Applicants' claimed invention of a self-authenticating document which, in part, depends on affixing the public key certificate and public key to the value document. Thus, Gordon clearly teaches away from Applicants' claimed invention, and the Examiner's arguments cannot stand.

IV. Conclusion

In view of the above-stated reasons and the previous arguments made in the May 16th Response and incorporated by reference herein, Applicants submit that claims 29-144 are allowable over the prior art of record, and that the application is in condition for allowance. It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests prompt and favorable consideration of this amendment and reconsideration of the application on whole. An early Notice of Allowance is also respectfully solicited. Should the Examiner believe that personal communication would

[THIS SPACE INTENTIONALLY LEFT BLANK]

expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (215) 986-5169.

Respectfully submitted,

BRUCE K. GEIST
THOMAS D. HAYOSH

BY: _____
Lise A. Rode
Attorney for Applicant
Reg. No. 37,226

Unisys Corporation
Unisys Way, M/S E8-114
Blue Bell, Pennsylvania 19424-0001

The Director for Patents is hereby authorized to charge payment to Deposit Account No. 19-3790 of any fees associated with this communication.

I hereby certify that this correspondence is being transmitted via facsimile ((703) 872-9306) to the United States Patent and Trademark Office on the date shown below.

September 21, 2005

_____